S 1?
ET
S-83132/PN

S 1 RESULT (1)

S 2?
ET
RT FU

1- (JAPIO)
N - 91-083132
I - SOFTWARE PROTECTION CONTROL SYSTEM
A - (2000522) FUJITSU LTD
N - AZUMA, MITSUHIRO; HASEBE, TAKAYUKI; MATSUMOTO, MASAMI; SONOHARA,
     SATOSHI
N - 91.04.09 J03083132, JP 03-83132
P - 89.08.28 89JP-218615, 01-218615
O - 91.06.27 SECT. P, SECTION NO. 1221; VOL. 15, NO. 255, PG. 81.
C - G06F-009/06
C - 45.1 (INFORMATION PROCESSING--Arithmetic Sequence Units)
KW - R131 (INFORMATION PROCESSING--Microcomputers & Microprocessers)
B - PURPOSE: To protect software by ciphering a decipher key of
     software with an individual key of a user to obtain assent
     information and enabling only a regular user to decipher the
     decipher key from assent information.
     CONSTITUTION: In a software managing part 1, an individual key of
     the regular user is generated by an individual key generating
     part 3 and is reported, and software of a normal text is ciphered
     with the decipher key by a software ciphering part 5 to obtain a
     ciphered text, and the decipher key is ciphered with the
     individual key by a key ciphering part 4 to obtain assent
     information. Ciphered text software and the decipher key ciphered
     as assent information are transferred to the user. Though
     software presented from the software managing part 1 is copied,
     deciphering and execution without the decipher key are impossible
     because it is ciphered, and thus, software is protected.

SS 2?

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平3-83132

⑤Int. Cl.[5]	識別記号	庁内整理番号	㊸公開　平成3年(1991)4月9日
G 06 F 9/06	450 C	7361-5B	

審査請求　未請求　請求項の数 1　(全7頁)

㊹発明の名称　ソフトウエア保護制御方式

㉑特　願　平1-218615
㉒出　願　平1(1989)8月28日

㉗発明者　東　充宏　神奈川県川崎市中原区上小田中1015番地　富士通株式会社内
㉗発明者　長谷部　高行　神奈川県川崎市中原区上小田中1015番地　富士通株式会社内
㉗発明者　松元　雅美　神奈川県川崎市中原区上小田中1015番地　富士通株式会社内
㉗発明者　苑原　聡　神奈川県川崎市中原区上小田中1015番地　富士通株式会社内
㉑出願人　富士通株式会社　神奈川県川崎市中原区上小田中1015番地
㉔代理人　弁理士　柏谷　昭司　外1名

明　細　書

1　発明の名称

ソフトウェア保護制御方式

2　特許請求の範囲

ソフトウェア管理部(1)に於いてソフトウェアを暗号化してユーザに提供し、該ソフトウェアをソフトウェア実行部(2)に於いて復号して実行するソフトウェア保護制御方式に於いて、

前記ソフトウェア管理部(1)の個別鍵生成部(3)に於いてユーザの個別鍵を生成し、該個別鍵によりソフトの復号鍵を鍵暗号化部(4)に於いて暗号化して許諾情報を形成し、且つ前記復号鍵によりソフトウェアをソフトウェア暗号化部(5)に於いて暗号化して提供し、

前記ソフトウェア実行部(2)の鍵復号化部(6)に於いて前記許諾情報を前記個別鍵により復号して前記復号鍵を形成し、該復号鍵により前記暗号化されたソフトウェアをソフトウェア復号化部(7)に於いて復号して実行する

ことを特徴とするソフトウェア保護制御方式。

3　発明の詳細な説明

〔概要〕

コンピュータの各種のソフトウェアの不正使用を防止するソフトウェア保護制御方式に関し、

正規のユーザのみが暗号化されたソウトウェアを復号して実行できるようにすることを目的とし、

ソフトウェア管理部に於いてソフトウェアを暗号化してユーザに提供し、該ソフトウェアをソフトウェア実行部に於いて復号して実行するソフトウェア保護制御方式に於いて、前記ソフトウェア管理部の個別鍵生成部に於いてユーザの個別鍵を生成し、該個別鍵によりソフトの復号鍵を鍵暗号化部に於いて暗号化して許諾情報を形成し、且つ前記復号鍵によりソフトウェアをソフトウェア暗号化部に於いて暗号化して提供し、前記ソフトウェア実行部の鍵復号化部に於いて前記許諾情報を前記個別鍵により復号して前記復号鍵を形成し、該復号鍵により前記暗号化されたソフトウェアをソフトウェア復号化部に於いて復号して実行するように構成した。

〔産業上の利用分野〕

本発明は、コンピュータの各種のソフトウェアの不正使用を防止するソフトウェア保護制御方式に関するものである。

コンピュータのソフトウェアの開発が、ハードウェアの開発を凌ぐ勢いで行われており、特に、パーソナルコンピュータ（以下パソコンと略称）用のソフトウェアは、多数のソフトウェアベンダーによって提供されるようになり、その種類も多数となっている。

しかし、ソフトウェアはハードウェアのような有体物ではなく、複製が容易なものであり、従って、新たに開発されたソフトウェアであっても、複製により正規のユーザ以外でも容易に利用することが可能となり、ソフトウェアベンダーの利益を守ることができないものであった。

そこで、ソフトウェアの正規のユーザのみが、そのソフトウェアを実行できるようにすることが要望されている。

〔従来の技術〕

パソコン用のソフトウェアの保護制御方式は、例えば、(1)ソフトウェアによる方式と、(2)ハードウェアを併用する方式と、(3)その他の方式に分けることができる。ソフトウェアによる方式(1)は、例えば、ソフトウェアが格納されたフロッピィディスク等の記憶領域の中で、ＯＳ（オペレーティング・システム）によりサポートするコマンドではコピーできない領域に、或る情報を書込んで置き、ソフトウェアの実行開始時に、その領域のデータを読出して、設定データと一致しない場合は実行できないようにする方式である。

又ハードウェアを併用する方式(2)は、拡張スロット等に専用のハードウェアをセットし、ソフトウェアの実行が可能か否かを判断させるもので、正規のユーザのみがそのソフトウェアを実行できるようにし、そのハードウェアがセットされていないパソコンは、当然にそのソフトウェアを実行できないものである。

又その他の方式(3)は、例えば、暗号化したソフトウェアの利用の条件を記述した許諾条件プログラムを設けて、許諾条件以外の条件の場合は、そのソフトウェアを実行できないようにした方式が提案されている。この方式については、電子通信学会論文誌，１９８７年１月，Ｖｏｌ．Ｊ７０－Ｄ，Ｎｏ．１，第７０頁～第８１頁の「ソフトウェア・サービス・システム（ＳＳＳ）の提案」及び電子通信学会論文誌，１９８７年２月，Ｖｏｌ．Ｊ７０－Ｄ，Ｎｏ．２，第３３５頁～第３４５頁の「ソフトウェア・サービス・システム（ＳＳＳ）の小規模な試作」の表題で説明されている。

〔発明が解決しようとする課題〕

前述の従来例のソフトウェアによる方式(1)は、ハードウェアによるコピーマシンを使用することにより、総ての領域のコピーが可能となることから、大量に複製できるという問題点があり、ソフトウェアの保護が充分でない欠点がある。

又ハードウェアを併用する方式(2)は、ソフトウェア保護用のハードウェアをユーザが購入しなければならないから、ユーザの負担が増加する欠点がある。

又その他の方式(3)として、許諾条件プログラムを設ける方式は、共通クレジット等を用いるものであるから、ソフトウェアの流通経路を変更する必要があり、又ソフトウェアの実行権を管理する為のＳＳＳＢＯＸと称する専用のハードウェアを必要とする欠点があり、装置の大型化とユーザの負担増との問題点がある。

本発明は、正規のユーザのみが暗号化されたソウトウェアを復号して実行できるようにすることを目的とするものである。

〔課題を解決するための手段〕

本発明のソフトウェア保護制御方式は、ソフトウェアの復号鍵をユーザの個別鍵で暗号化して許諾情報とし、正規のユーザのみがその許諾情報から復号鍵を復号できるようにしたものであり、第１図を参照して説明する。

ソフトウェア管理部１に於いてソフトウェアを暗号化してユーザに提供し、そのソフトウェアをソフトウェア実行部２に於いて復号して実行する

ソフトウェア保護制御方式に於いて、ソフトウェア管理部1の個別鍵生成部3に於いてユーザの個別鍵を生成し、この個別鍵により復号鍵を鍵暗号化部4に於いて暗号化して許諾情報とし、且つ復号鍵によりソフトウェアをソフトウェア暗号化部5に於いて暗号化してユーザに提供する。

ユーザは、ソフトウェア実行部2の鍵復号化部6に於いて許諾情報を個別鍵により復号して復号鍵を形成し、この復号鍵を用いて暗号化されたソフトウェアをソフトウェア復号化部7に於いて復号して実行するものである。

〔作用〕

ソフトウェア管理部1に於いては、正規のユーザに対する個別鍵を個別鍵生成部3に於いて生成して通知し、又平文のソフトウェアをソフトウェア暗号化部5に於いて復号鍵で暗号化して暗号文とし、又その復号鍵を個別鍵で鍵暗号化部4に於いて暗号化して許諾情報とする。そして、ユーザには、暗号文ソフトウェアと、許諾情報として暗号化された復号鍵とが渡されることになる。

従って、ソフトウェア管理部1から提供されたソフトウェアを複製したとしても、暗号化されているから、復号鍵がないと復号して実行することができないことになり、ソフトウェアを保護することができる。

又正規のユーザは、個別鍵を用いて鍵復号化部6に於いて許諾情報を復号して復号鍵を得ることができるから、その復号鍵を用いて暗号文のソフトウェアをソフトウェア復号化部7に於いて平文のソフトウェアに復号して実行することになり、正規のユーザのみがそのソフトウェアを実行できることになる。

〔実施例〕

以下図面を参照して本発明の実施例について詳細に説明する。

第2図は本発明の実施例のソフトウェア管理部の説明図であり、11はフロッピィディスク等に格納された平文のソフトウェア、12は暗号化処理部、13は書込部、14はコンパクトディスク（CD）等に格納された暗号文のソフトウェア、15は暗号化処理部12に加える暗号鍵（ユーザ側の復号鍵）を発生する乱数発生部、16はソフトウェア名と暗号鍵とを対応させて登録する鍵管理テーブル部、17はユーザの識別情報IDからユーザの個別鍵を生成するユーザ個別鍵生成部、18は暗号鍵を個別鍵で暗号化して許諾情報を形成する許諾情報生成部、19はバリデーション・ディスク、20はバリデーション・ディスク19内のバリデーション・テーブル部である。

暗号化処理部12が第1図のソフトウェア暗号化部5に対応し、ユーザ個別鍵生成部17が第1図の個別鍵生成部3に対応し、又許諾情報生成部18が第1図の鍵暗号化部4に対応する。

ソフトウェアベンダー等によって作成された平文ソフトウェア11は、暗号化処理部12に於いて暗号化される。その場合の暗号鍵は乱数発生部15からの乱数が用いられる。又暗号化方式は、例えば、DES（Data Encryption Standard）等の慣用暗号方式を用いることができる。このDES方式は、64ビットのデータブロック毎に暗号化及び復号化を行うもので、鍵の長さは56ビットであり、それに8ビットのパリティビットが付加されるものである。

暗号化処理部12によりソフトウェアが暗号化され、書込部13によりフロッピィディスクやコンパクトディスク（CD）等に書込まれて、暗号文ソフトウェア14としてユーザに提供される。コンパクトディスク（CD）を用いた場合は、記憶容量が非常に大きいので、複数種類の暗号文ソフトウェアを書込むことができる。

又鍵管理テーブル部16に、乱数発生部15からの暗号鍵と、暗号化するソフトウェア名とが対応して登録されるものであり、例えば、図示の場合、ソフトウェア名「TOWNS PAINT」と、それに対応する64ビット長の暗号鍵が16進表示で「2F6E894D3CE08DAC」として登録され、同様に、ソフトウェア名「TOWNS VNET」と、それに対応する64ビット長の暗号鍵が16進表示で「983ECA56E7F8E781」として登録されている。

ユーザが例えばソフトウェア名「ＴＯＷＮＳ　ＰＡＩＮＴ」のソフトウェアを購入する場合、ユーザのパソコンの識別情報ＩＤを基に、ユーザ個別鍵生成部１７により個別鍵が生成される。この個別鍵は、ユーザ側のソフトウェア実行部２に個別鍵生成部を有しない場合は、この個別鍵を厳重に管理してユーザに引き渡すことになる。そして、この個別鍵を用いて、許諾情報生成部１８に於いてソフトウェア名「ＴＯＷＮＳ　ＰＡＩＮＴ」の暗号鍵が暗号化されて許諾情報となる。この許諾情報は、バリデーション・ディスク１９のバリデーション・テーブル部２０に登録される。即ち、図示のように、暗号文ソフトウェアのソフトウェア名「ＰＡＩＮＴ　．ＥＮＣ」とその許諾情報「５２２Ｅ３ＡＢＣ４５３Ｆ２Ｅ９Ａ」とが登録され、このバリデーション・ディスク１９はユーザに引き渡される。

第３図は本発明の実施例のソフトウェア管理部の処理フローチャートを示し、ソフトウェア暗号化処理か許諾情報発行処理かを判定し①、ソフトウェア暗号化処理の場合は、乱数発生部１５から乱数を発生させ②、その乱数を暗号鍵として、鍵管理テーブル部１６に登録し③、その暗号鍵を用いてソフトウェアを暗号化処理部１２に於いて暗号化し④、書込部１３に於いて暗号文のソフトウェアの書込みを行う⑤。

又許諾情報発行処理の場合は、鍵管理テーブル部１６を参照して⑥、ソフトウェア名に対応する暗号鍵を読出し、又ユーザ個別鍵生成部１７に於いてユーザの識別情報ＩＤを基に個別鍵を生成し⑦、この個別鍵を用いて暗号鍵を暗号化して、バリデーション・テーブル部２０に登録し⑧、これを許諾情報としてユーザに発行する⑨。

第４図は本発明の実施例のソフトウェア実行部の説明図であり、２１はソフトウェア管理部から発行されたバリデーション・ディスク（第２図の符号１９に対応）、２２はバリデーション・テーブル部、２３は許諾情報登録部、２４はユーザ用バリデーション・ディスク、２５はユーザ用バリデーション・テーブル部、２６はユーザ個別鍵生成部、２７は鍵復号化部、２８は復号化処理部、２９は暗号文ソフトウェア（第２図の符号１４に対応）、３０は平文ソフトウェア、３１は実行部である。

許諾情報登録部２３とユーザ用バリデーション・テーブル部２５とユーザ個別鍵生成部２６と鍵復号化部２７と復号化処理部２８と実行部３１とは、ユーザの例えばパソコンの処理機能によって実現することができるものである。

又バリデーション・ディスク２１のバリデーション・テーブル部２２は、第２図に於けるバリデーション・ディスク１９のバリデーション・テーブル部２０に対応し、例えば、暗号化されたソフトウェア名の「ＰＡＩＮＴ　．ＥＮＣ」と、それに対応した許諾情報とが書込まれており、許諾情報登録部２３に於いてユーザ用バリデーション・ディスク２４のユーザ用バリデーション・テーブル部２５に、暗号文ソフトウェアのソフトウェア名とその許諾情報とが追加登録される。

このユーザ用バリデーション・テーブル部２５に於いて、ソフトウェア名「ＦＢ３８６　．ＥＮＣ」，「ＶＮＥＴ　．ＥＮＣ」，「ＳＯＵＮＤ　．ＥＮＣ」のソフトウェアをユーザが購入したことにより、そのソフトウェア名とその許諾情報とが既に登録され、今回購入したソフトウェアのソフトウェア名「ＰＡＩＮＴ　．ＥＮＣ」とその許諾情報とが、バリデーション・テーブル部２２から読出されて、ユーザ用バリデーション・テーブル部２５に登録された場合を示すものである。

又ユーザの識別情報ＩＤを基にユーザ個別鍵生成部２６に於いて個別情報が生成される。この機能を有しない場合は、ソフトウェア管理部１から個別鍵を厳密な管理下で受け取ることになる。そして、これから実行するソフトウェア名をユーザが指定すると、バリデーション・テーブル部２５から指定ソフトウェア名に対応する許諾情報が読出されて、鍵復号化部２７に加えられ、ユーザの個別鍵により許諾情報が復号されて復号鍵が形成される。そして、この復号鍵により指定ソフトウェアが復号化処理部２８に於いて復号されて、平

文ソフトウェア30となり、実行部31に於いて実行されることになる。この復号化処理は、実行部31に於いて実行するステップ毎等に対応して順次行われるものである。

第5図は本発明の実施例のソフトウェア実行部の処理フローチャートを示し、許諾情報登録の処理か実行かを判定し⑪、許諾情報登録処理の場合は、ユーザ用バリデーション・テーブル部25に許諾情報を登録する⑫。又実行の場合は、指定ソフトウェア名に対応する許諾情報が登録されているか否かの許諾チェックを行い⑬、許諾情報が登録されていない場合は不許可となる。又登録されている場合は、ユーザ個別鍵生成⑭、個別鍵による許諾情報の復号による鍵復号⑮を行い、指定ソフトウェアを復号鍵によって復号し⑯、そのソフトウェアを実行する⑰。

ソフトウェアは、全部のステップを総て暗号化することも可能であるが、重要なステップのみを暗号化することも可能である。その場合は、復号化処理が容易となる。又バリデーション・ディスク19，21のバリデーション・テーブル部20，22は、フロッピィディスク以外の手段でもユーザに引き渡すこともできるものであり、例えば、パソコン通信網を利用してユーザに通知することもできる。

〔発明の効果〕

以上説明したように、本発明は、ソフトウェア管理部1の個別鍵生成部3により個別鍵を生成し、鍵暗号化部4により個別鍵を用いて復号鍵を暗号化して許諾情報とし、ソフトウェア暗号化部5によりソフトウェアを復号鍵を用いて暗号化し、ユーザ側では、ソフトウェア実行部2の鍵復号化部6により、許諾情報を個別鍵により復号して復号鍵を形成し、ソフトウェア復号化部7により暗号文ソフトウェアを復号して実行するものであり、ソフトウェアは暗号化されていると共に、その復号鍵も、ユーザの個別鍵により暗号化されているから、ソフトウェアを複製しても、正規のユーザ以外は、許諾情報から復号鍵を得ることができないので、そのソフトウェアを実行できないことになる。即ち、ソフトウェアを保護することができる。

又許諾情報の登録や復号化をOSでサポートすることは容易であり、従って、ユーザは特別なハードウェアを必要としないから、負担が増加することはない。

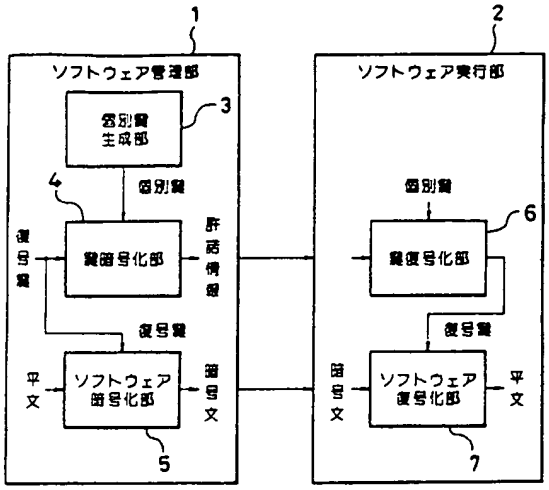
又大容量のメディア（コンパクトディスク等）に、複数種類の暗号化したソフトウェアをまとめて書込んでおき、その中でユーザが購入するソフトウェアについてのみ、それに対応する許諾情報を発行することができるから、ソフトウェアの流通コストを低減することが可能となる。又ソフトウェア管理部1に於いて、許諾情報の発行を管理することが容易であるから、簡単にユーザの動向を知ることができる。

4　図面の簡単な説明

第1図は本発明の原理説明図、第2図は本発明のソフトウェア管理部の説明図、第3図は本発明のソフトウェア管理部の処理フローチャート、第4図は本発明の実施例のソフトウェア実行部の説明図、第5図は本発明の実施例のソフトウェア実行部の処理フローチャートである。

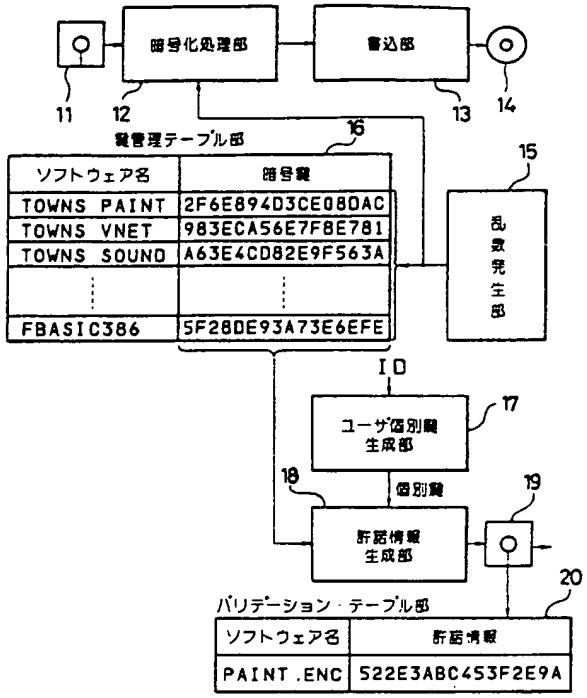
1はソフトウェア管理部、2はソフトウェア実行部、3は個別鍵生成部、4は鍵暗号化部、5はソフトウェア暗号化部、6は鍵復号化部、7はソフトウェア復号化部である。

特許出願人　富士通株式会社
代理人弁理士　柏谷昭司
代理人弁理士　渡邊弘一



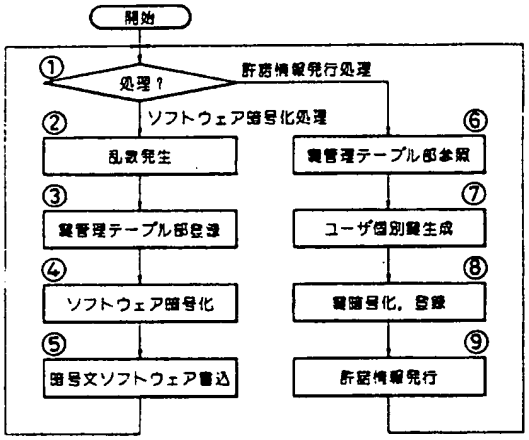
本発明の原理説明図

第 1 図



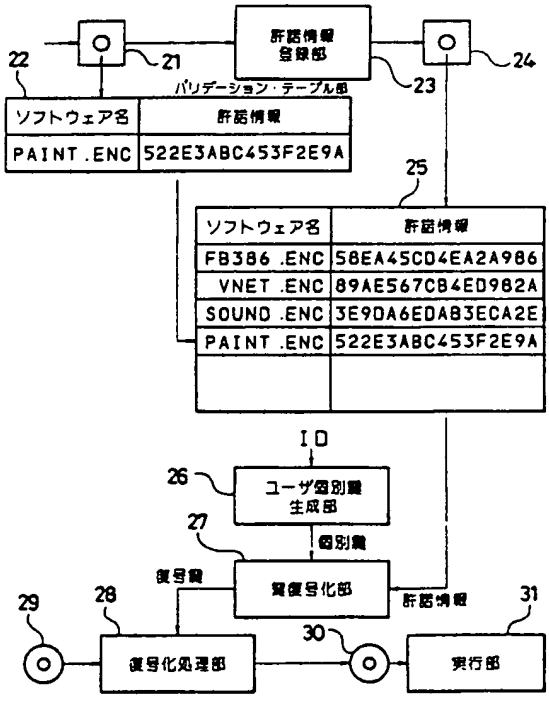
本発明の実施例のソフトウェア管理部の説明図

第 2 図



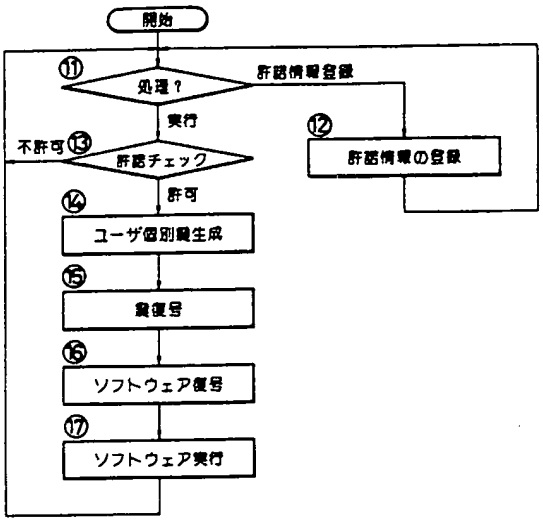
本発明の実施例の
ソフトウェア管理部の処理フローチャート

第 3 図



本発明の実施例のソフトウェア実行部の説明図

第 4 図



本発明の実施例の
ソフトウェア実行部の処理フローチャート
第 5 図